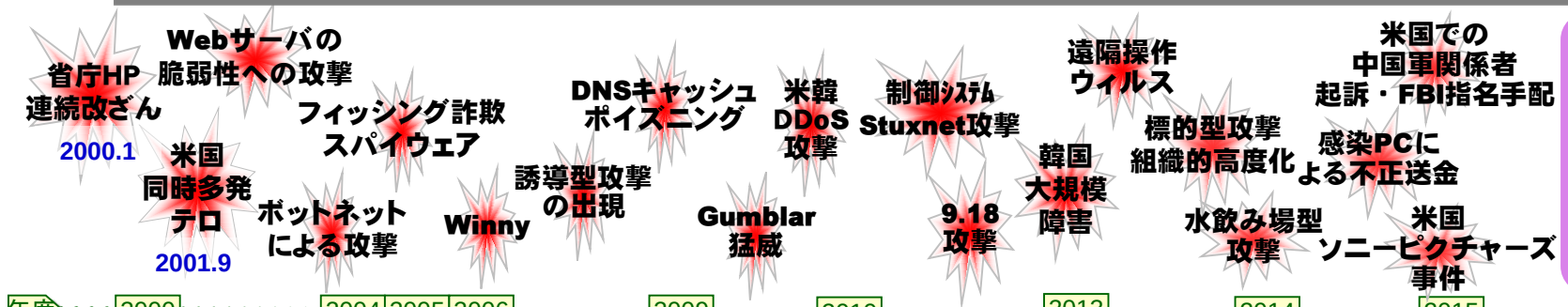
資料４

新・サイバーセキュリティ戦略について

サイバーセキュリティ政策の経緯



○今後の重要な環境変化
- オリンピック・パラリンピック東京大会
- マイナンバー利用開始
- IoTの広がり　等
  （スマートメーター、自動走行システム等）

情報セキュリティ・サイバーセキュリティ

- 第１次 情報セキュリティ基本計画（2006.2.2）情報セキュリティ政策会議決定
- 第２次 情報セキュリティ基本計画（2009.2.3）情報セキュリティ政策会議決定
- 国民を守る情報セキュリティ戦略（2010.5.11）情報セキュリティ政策会議決定
- サイバーセキュリティ戦略（2013.6.10）情報セキュリティ政策会議決定
- サイバーセキュリティ基本法公布（2014.11.12）
- **新・サイバーセキュリティ戦略（2015.X.XX）サイバーセキュリティ戦略本部決定 閣議決定**

IT利活用

- e-Japan戦略（2001.1）
- e-Japan戦略Ⅱ（2003.7）
- IT新改革戦略（2006.1）
- i-Japan戦略2015（2009.7）
- 新たな情報通信技術戦略（2010.5）
- 世界最先端ＩＴ国家創造宣言（2013.6.14 IT総合戦略本部決定・閣議決定, 2014.6.24 改訂）
  - サイバーセキュリティ立国」の実現が急務

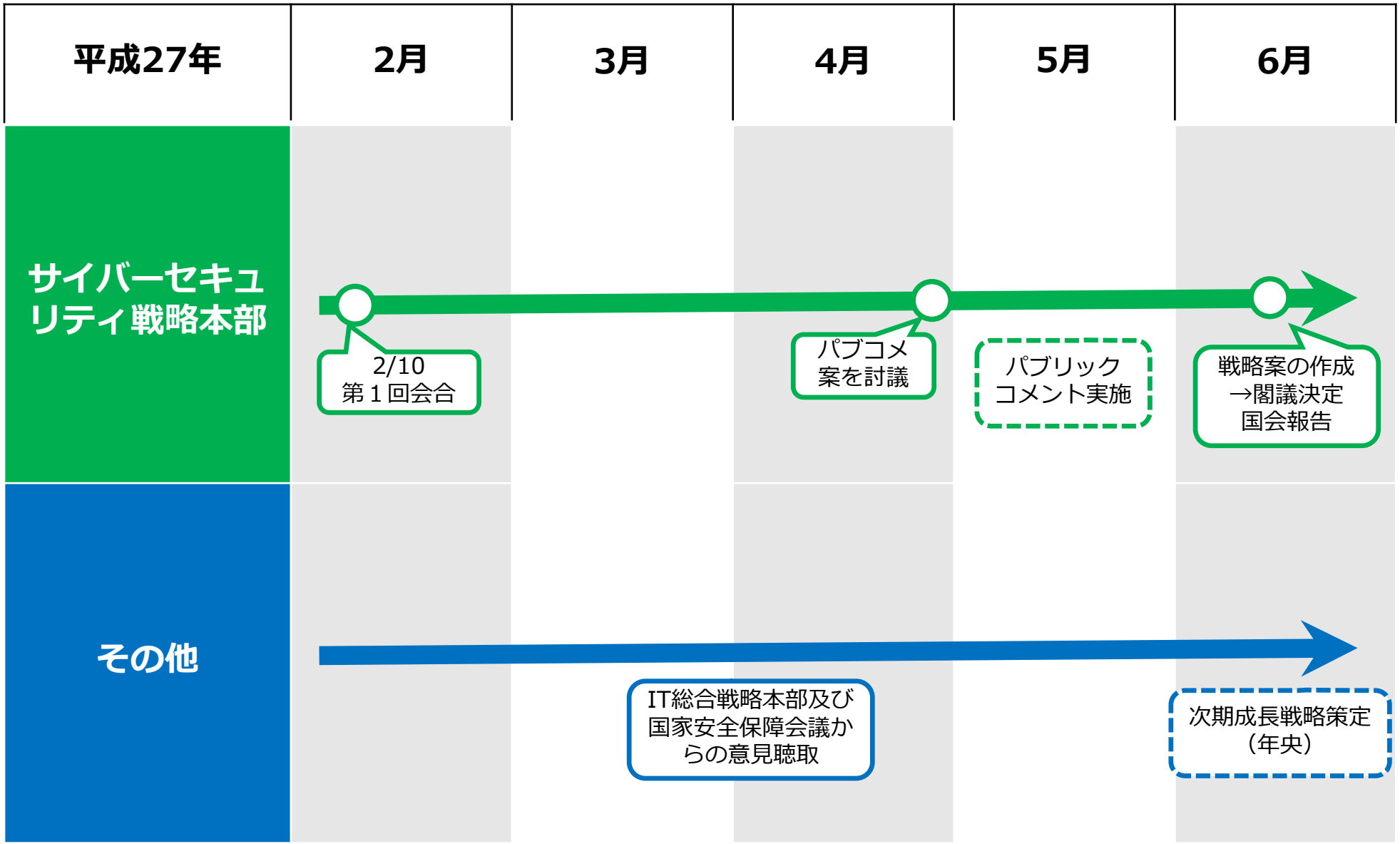
安全保障

- 国家安全保障戦略（2013.12.17 閣議決定）
  - サイバー空間の防護は、我が国の安全保障を万全とするとの観点から、不可欠

成長戦略

- 日本再興戦略（2013.6.10 閣議決定, 2014.6.24　改訂）
  - 「サイバーセキュリティ推進体制等の強化」が項目の一つ

今後の進め方（イメージ）


平成27年
2月
3月
4月
5月
6月
サイバーセキュリティ戦略本部
2/10
第１回会合
パブコメ
案を討議
パブリック
コメント実施
戦略案の作成
→閣議決定
国会報告
その他
IT総合戦略本部及び
国家安全保障会議か
らの意見聴取
次期成長戦略策定
（年央）

主な検討課題

【全般的事項】

・今後、「サイバー空間」はどのような性質の空間として発展していくと考えるか。

・サイバー空間における多様な主体間の役割分担をどのように考えていくべきか。

・サイバーセキュリティ政策を推進する上で、我が国はどのような基本原則に基づくべきか。

【政策分野別事項】

・サイバー空間を通じて我が国の経済・社会の持続的な発展を実現するためには、サイバーセキュリティが果たす役割や必要とされる政策をどのように考えるか。

・国民が、サイバー空間上で安全に、安心して豊かな経済社会活動を行うためにはどのような対策が必要か。

・サイバー空間に係る我が国の安全保障を確保し、国際社会の平和に貢献するためには、どのような政策を追求すべきか。

【基盤的事項】

・社会全体のセキュリティ意識を高め、更にその能力を高めるためには、どのような取組が考えられるか。

・日本におけるセキュリティ人材を充実させるためには、どのような政策を推進すべきか。

・社会や技術が変化していく中、サイバーセキュリティに関する研究開発等はどのようなあり方が適切か。

【参考】

本戦略の位置付け

サイバーセキュリティ基本法（平成26年法律第104号）（抄）

第十二条　政府は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティに関する基本的な計画（以下「サイバーセキュリティ戦略」という。）を定めなければならない。

２　サイバーセキュリティ戦略は、次に掲げる事項について定めるものとする。

一　サイバーセキュリティに関する施策についての基本的な方針

二　国の行政機関等におけるサイバーセキュリティの確保に関する事項

三　重要社会基盤事業者及びその組織する団体並びに地方公共団体（以下「重要社会基盤事業者等」という。）におけるサイバーセキュリティの確保の促進に関する事項

四　前三号に掲げるもののほか、サイバーセキュリティに関する施策を総合的かつ効果的に推進するために必要な事項

３　内閣総理大臣は、サイバーセキュリティ戦略の案につき閣議の決定を求めなければならない。

４　政府は、サイバーセキュリティ戦略を策定したときは、遅滞なく、これを国会に報告するとともに、インターネットの利用その他適切な方法により公表しなければならない。

５・６　（略）

（所掌事務等）

第二十五条　本部は、次に掲げる事務をつかさどる。

一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。

二～四　（略）

２　本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、高度情報通信ネットワーク社会推進戦略本部及び国家安全保障会議の意見を聴かなければならない。

３・４　（略）

各国のサイバーセキュリティ戦略等について

【参考】

国名等	サイバーセキュリティ戦略等について				備考
	策定年	戦略目的	サイバー空間とは	原則	
 アメリカ	2011年 ホワイトハウス 「サイバー空間に係る国際戦略」	国際商取引を支え、国際的な安全を強化し、表現の自由とイノベーションを育む情報通信基盤を国際協調の下に拡大する	経済の繁栄、活発な研究、強い軍事力、透明な政府そして自由な社会の屋台骨	基本的自由・プライバシー・情報の自由な流通の保護	・2014年末にサイバーセキュリティ関連の法律が数本成立。国土安全保障省の位置づけの明確化、国家サイバーセキュリティ・通信統合センター（NCCIC）の法制化等が内容。
	2011年 国防総省 「サイバー空間活動戦略」	米国及び同盟国のサイバー空間での活動能力に対するリスクを低減すること		プライバシー・市民的自由・表現の自由・イノベーションの尊重	
	2011年 国土安全保障省 「国土安全保障企業のためのサイバーセキュリティ戦略」	安全で強靭なインフラであり、イノベーションと繁栄を可能にし、プライバシーと市民的自由を保護するように設計されたサイバー空間を目指す	インターネット、通信ネットワーク、コンピュータシステム及び重要産業における組み込みプロセッサやコントローラ等を含むITインフラの相互依存ネットワーク	プライバシーと市民的自由／透明性／分散した主体間での責任共有／リスクベース・費用効率的・判断可能なセキュリティ	
 ＥＵ	2013年 「EUサイバーセキュリティ戦略」	全ての人々の利益のため、最大限の自由と安全を提供し、オンライン環境を保護		物理空間と同様の価値の適用／基本的人権・表現の自由・個人情報・プライバシーの保護／自由なアクセス／民主的・効率的なマルチステークホルダーによる支配／責任の共有体制	・サイバーセキュリティ指令案が欧州議会を通過。（理事会未承認）
 ドイツ	2011年 「サイバーセキュリティ戦略」	経済・社会的繁栄の維持、促進	データ層にリンクされた全てのITシステムにより構成される世界規模の仮想空間	情報共有・協力ベースの総合的アプローチ／民間活力の重視／国際協調	・「Industrie4.0」（インダストリー4.0）として、IoTによる製造業の技術革新を提唱。
 フランス	2011年 「情報システム防護・セキュリティ戦略」	サイバー防衛大国となること／情報保全を通じ、主権に関する意思決定能力を保持すること／重要インフラのセキュリティを強化すること／サイバー空間のセキュリティ確保すること	世界の文化が共有され、アイディアや情報が即時に流通し、個々人が議論する空間		・国家情報システム・セキュリティ庁（ANSSI)の体制を、2015年までに現在の350名から500名に拡充。
 イギリス	2011年 「サイバーセキュリティ戦略」	経済的、社会的価値の享受	情報を保存、変更、通信するために使用されるデジタルネットワークで構成される双方向の領域	自由／公正／透明／法の支配	・オリンピックを契機にCERT-UKを設立する等、体制強化を推進。

※　NISC調べ